



**Industry**  
Healthcare

**VMware footprint**  
VMware NSX-T™

**VMware partner**  
SPJ Solutions

### Key challenges

- Managing network security policies across multiple VMware vCenter® sites was time-consuming using VMware NSX Data Center for vSphere®.
- The inability to apply network policies centrally increased security oversights and policy inconsistencies.
- Complex infrastructure and very low tolerance for downtime made planning a migration to NSX-T challenging.

### Solution

- NSX-T federation centralizes network policies and applies them consistently across all vCenter sites.
- A carefully planned, custom migration process, with support from VMware and a VMware consulting partner, enabled a zero-downtime migration to NSX-T.

### Operational benefits

New network policies can be deployed within days, instead of weeks.

# Major Healthcare Network Achieves a Zero-Downtime Migration to VMware NSX-T

For years, a large, U.S.-based healthcare network had been using VMware NSX Data Center for vSphere to connect and protect thousands of hosts spread across more than a dozen sites. Those virtual machines (VMs) powered several mission-critical apps, which clinicians relied on to deliver lifesaving treatments. They also supported systems that managed patient information, scheduled healthcare interventions, and more.

Today, the company has migrated to VMware NSX-T, which simplifies network security policy management and offers additional features not available in NSX Data Center for vSphere. However, migrating to the newer platform was no simple task, given the complexity of the company's infrastructure and the fact it could not tolerate any downtime for many of its workloads.

Here's how the company navigated the migration to NSX-T, as well as the benefits it has reaped by making the change.

### The challenge

The company's healthcare network depends on more than 10,000 VMs running across more than a dozen physical sites. Each physical site is managed via a dedicated VMware vCenter instance.

The company's IT team was able to manage this infrastructure well enough using NSX Data Center for vSphere, but they lacked operational efficiency. This was because, with NSX Data Center for vSphere, each vCenter instance in the company's infrastructure had its own NSX Manager™. As a result, whenever the IT organization wanted to create a new network security policy, it had to deploy the policy separately at each vCenter instance. This manual process became time consuming and, it also created potential security risks and inconsistencies within network security rules.



“Occasionally, a controller that did not get set up correctly would get missed, for example,” an IT lead at the healthcare network said. “It could also be challenging to keep up with the cross-synchronization of security policies.”

NSX-T federation solves this problem by allowing security policies to be deployed through a centralized global manager. There’s no need to apply a separate policy for each vCenter instance. At the same time, NSX-T includes advanced network management features, such as support for complex IP management and load balancing, that are not available in NSX Data Center for vSphere, but that the company wanted to leverage to improve the efficiency of its networks.

The company decided to migrate to NSX-T. Yet, the challenge was to determine how to perform the migration without risking downtime.

“Having 100 percent uptime is key for our clinicians to be able to best provide care for our patients,” the IT lead said. He added that the considerable scale of the company’s infrastructure, combined with its multisite architecture, made it especially challenging to plan a migration process that would minimize risk.

## The solution

To address these migration challenges, the company worked closely with VMware and SPJ Solutions, a VMware consulting partner. cITopus, a technology developed by SPJ Solutions, was used to migrate company’s NSX-V environment to NSX-T.

To start the process, “VMware came out and visited us in person to map out our requirements,” said the IT engineer. VMware engineers recognized early on that, what they referred to as a big-bang migration—meaning the migration of all clusters from NSX Data Center for vSphere to NSX-T in a single go—wasn’t feasible given the complex nature of the company’s infrastructure and its very low tolerance for downtime risk.

VMware and SPJ collaborated with the company to map out and implement a more nuanced migration process. The plan centered on migrating the clusters to NSX-T one by one, starting with clusters that hosted the least-critical workloads. In addition, a variety of pre- and post-migration tests were set up so that NSX-T functionality could be carefully validated before and after each cluster migration took place. cITopus In-Place Migration Utility was used to perform migration of all components of NSX-V, including clusters, ESXi hosts, virtual machines, and Micro-segmentation.

The plan was a success. “The migration was a 100 percent success,” said the IT lead. “We didn’t have any downtime, and we were able to meet all the requirements we had laid out at the beginning of the project.”

He added that the migration technology, cITopus, and migration process that SPJ provided helped ensure that the company’s environment continued to operate smoothly, even during the migration, when some clusters remained on NSX Data Center for vSphere and others had been migrated to NSX-T.



## Operational results and benefits

With all clusters now fully migrated to NSX-T, the healthcare network enjoys a substantial reduction in operational overhead related to NSX policy management.

Previously, it took two to three weeks for an engineer to apply a single policy, which translated to a major operational burden, given that the company has hundreds of applications that need to be micro-segmented using network policies. Subsequently, that process has been reduced to a matter of days, adding enormous efficiency.

As a result, because it takes much less time to set up network policies, the company has been able to increase the number of applications that it secures using micro-segmentation. Previously, it had not been feasible to micro-segment every application due to the time required to manage network policies. Today, full micro-segmentation is within reach.

This means that the security of the company's network is stronger than ever. "We have improved our capability to provide a secure infrastructure to run our mission-critical applications," the IT lead said.

## Future plans

A more efficient policy management process is only the first key benefit that the company has reaped through its migration to NSX-T.

Its engineers are now also in the early stages of taking advantage of the NSX-T overlay and enhanced load balancing features to improve the overall efficiency of its networks. And going forward, NSX-T will make it easier to deploy cloud native applications, which are not yet widespread in the healthcare industry but will likely be in the future.

"We are starting to look at what we need to do to support containers in our environment," the IT lead explained. "We don't see a lot of containers yet in healthcare, but we want to make sure we have the capability to support those workloads in the future." For this company, NSX-T is an important part of that equation.

## Learn more

For more information about migrating to VMware NSX-T, visit [vmware.com/go/v2t](https://vmware.com/go/v2t).

## For more help on migrations

Assess your environment for migration using the [migration assessment tool](#). For any additional help, contact a [VMware migration specialist](#).